EVOLVE IP

THE CLOUD STRATEGY COMPANY™

NORSTAR NETWORKS

DISASTER RECOVERY PLAN TEMPLATE

NORSTAR Networks | bflanagan@norstar.net | www.norstar.net | (579) 908-6000

Disaster Recovery Template: A Blueprint for Recovery

A Disaster Recovery Plan (DR Plan) is a detailed IT document that provides a blueprint for recovering from common IT-based business disruptions such as:

- Ransomware or Other Cyberattacks
- Environmental Catastrophes
- Building Accessibility or Power Disruption
- Employee Errors
- Hardware Failures
- Software Failures

Whether you are managing your DR plan internally or are entrusting your plan to a managed service provider, the document must contain detailed, accurate and up-to-date information about the IT operations of your organization. The DR Plan must present that information in a clear and coherent format that is easily consumable and – most importantly – actionable during an actual emergency. Your employees or service provider must be able to follow the document and react rapidly so that availability can be restored per the company’s established service level requirements.

Evolve IP designed this template to help our Disaster Recovery as a Service (DRaaS) clients – both infrastructure only clients and those leveraging our managed DRaaS services -- with the process of capturing and organizing the critical information needed to ensure that IT operations are in a position to survive when a disruption occurs.

This template is meant as a guide only. You should review it carefully to determine whether it appropriately fits your needs. If desired, our services team can guide you through the process to customize the template or create a comprehensive DR plan that best meets your own requirements and goals.

Protect with Prem Extend™: DRaaS Solutions from Evolve IP

A disaster recovery plan is no longer enough. Many businesses need data protection and automated options for business continuity. Evolve IP’s Prem Extend™ suite of Disaster Recovery as a Service (DRaaS) solutions help customers apply this same Disaster Recovery Plan template concept, but designing it to include a wide and powerful range of cloud-based backup and recovery solutions.

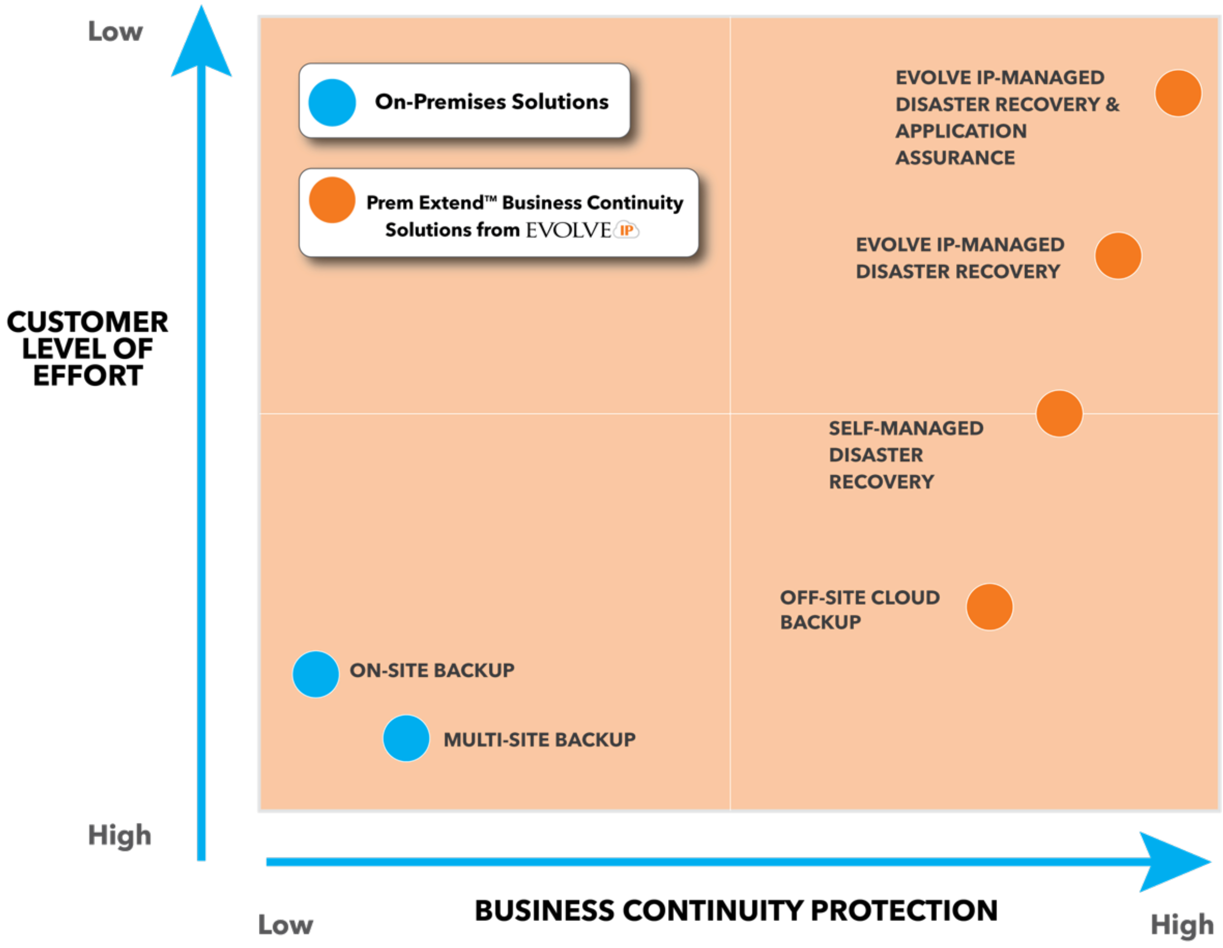
We help customers “extend” their on-premises business continuity protections into our secure Compliance Cloud™ - a PCI and HIPAA compliant computing environment built on the best-of-breed technology in our Infrastructure as a Service (IaaS) platform.

Our Prem Extend™ solutions have been carefully developed to provide cost effective, dependable options for customers to protect their critical business data and ensure recoverability. These cloud-based services provide customers with unmatched data loss prevention and the flexibility to address any RTO and RPO objectives. Driven by each customer’s unique needs, our DRaaS solutions offer backup and recovery protection for:

- **Desktops**
- **Physical Servers**
- **Operating Systems**
- **Hypervisors**
- **Storage**

We've designed our Prem Extend™ suite to allow businesses to determine their level of risk and spend accordingly. Our customers not only know where their data is backed up, they also know how and when they will have it restored when a disaster is declared, as defined in their Disaster Recovery Plan.

Evolve IP Prem Extend^{TM} Suite of Disaster Recovery and Business Continuity Solutions



Testing: Are You Truly Recoverable?

An essential component of our Prem Extend™ solutions – and of any disaster preparedness and recoverability plan – is testing. The DR Plan testing process should be conducted on a regular basis to ensure that all aspects of the plan are in fact practical and effective, and that all key personnel and resources are capable of performing as required to return the business availability under fire. Key questions answered by a comprehensive DR Plan include:

- Are employees and service providers able to execute the plan?
- Are data backups accessible within the desired timeframes?
- Are contingencies in place to adapt to accommodate resources or employees that may not be able to participate in the recovery process due to the disaster itself?
- Can the recovery time objective (RTO) practical or attainable?
- Can the systems be restored with an acceptable degree of data loss? Is the businesses recovery point objective (RPO) practical/attainable?

Instructions for Using This Template

This template can be used as a guide to compose a self-created DR Plan for your organization. To do so, complete all required sections and delete all unnecessary sections, replacing example text and Find and Replace text during the process. Once you have completed all sections, delete all instructional text (including this instruction page) as well as all "Required" or "Optional" markers and Find and Replace markers. Update the Table of Contents (right click and select "Update Fields") and then publish.

Content Key

Orange Text = "instructional text". When completing the template please review all instructional text to ensure complete understanding of the purpose of each section.

Italicized Text = "examples"*.* These examples are provided as guidance on to how to complete a section and supplement the information provided in the instructional text. In some cases example text (e.g. bullet lists) may be used as-is, added to, or deleted, while in other cases (e.g. sample table entries) it should be replaced with accurate, organization-specific information.

Required Text = it is probable that all organizations will need to retain and complete this section.
Optional Text = it is likely that only some organizations will need to include this section.

This template also includes time-saving placeholders for you to use with the *Find and Replace* function to insert the suitable information. These fields are delineated with brackets, like this: **{**this**}**. Simply enter each specific term with brackets in the *Find* field and the appropriate term in the *Replace* field.

Putting the Plan into Action

Once this document has been completed, you need to provide copies to all stakeholders (internal and/or external) and all associates or service providers who have responsibilities in the plan. You should create additional hard- and soft-copies for each data center or availability zone that houses your IT systems, including any standby or recovery facilities you have. You will need to ensure that the access to these hard and soft copies is protected to guarantee the integrity of the document.

Additionally, you should schedule time to review the document on a regular basis and to establish periodic tests to ensure continued applicability.

TABLE OF CONTENTS

INTRODUCTION

Required

This Disaster Recovery Plan (DR Plan) is the single source for all of the information that describes {Organization's Name}'s ability to survive a disaster including the processes that must be followed to accomplish disaster recovery.

Edit this section to suit your organization's needs, making all lists and other copy relevant to your organization.

DEFINITION: DISASTER

Optional

A disaster can be caused by many events resulting in {Organization Name}'s IT department not being able to perform some or all of their regular roles and responsibilities for a period of time. {Organization Name} defines disasters as the following:

- Edit this list to reflect your organization
- *One or more vital systems are non-functional*
- *The building is not available for an extended period of time but all systems are functional within it*
- *The building is available but all systems are non-functional*
- *The building and all systems are non-functional*

The following events can result in a disaster, requiring this DR document to be activated:

- Edit this list to reflect your organization
- *Environmental disaster (flooding, hurricane, fire, etc.)*
- *Hardware failure / server room issue*
- *Power outage*
- *Theft*
- *Deliberate attack*
- *Terrorist attack*
- *Human error*

THE PURPOSE OF THE DR PLAN

Required

The purpose for this DR Plan document is to inventory all of the IT infrastructure and capture all of the information relevant to the organization's ability to recover its IT from a disaster, and document the steps that the organization will follow in the event that a disaster occurs.

The top priority of {Organization Name} will be to enact the steps outlined in this DR Plan to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- Edit this list to reflect your organization
- *Preventing the loss of the organization's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the business running in the event of a disaster*

This DR Plan will also detail how this document is to be maintained and tested.

EMERGENCY CONTACT FORM

First Name	Last Name	Title	Contact Type	Contact information
Employee F	*Employee L*	*Title*	Work	*555-555-5555 ext. 555*
			Mobile	
			Alternate	
			Email	
			Work	
			Mobile	
			Alternate	
			Email	
			Work	
			Mobile	
			Alternate	
			Email	
			Work	
			Mobile	
			Alternate	
			Email	
			Work	
			Mobile	
			Alternate	
			Email	

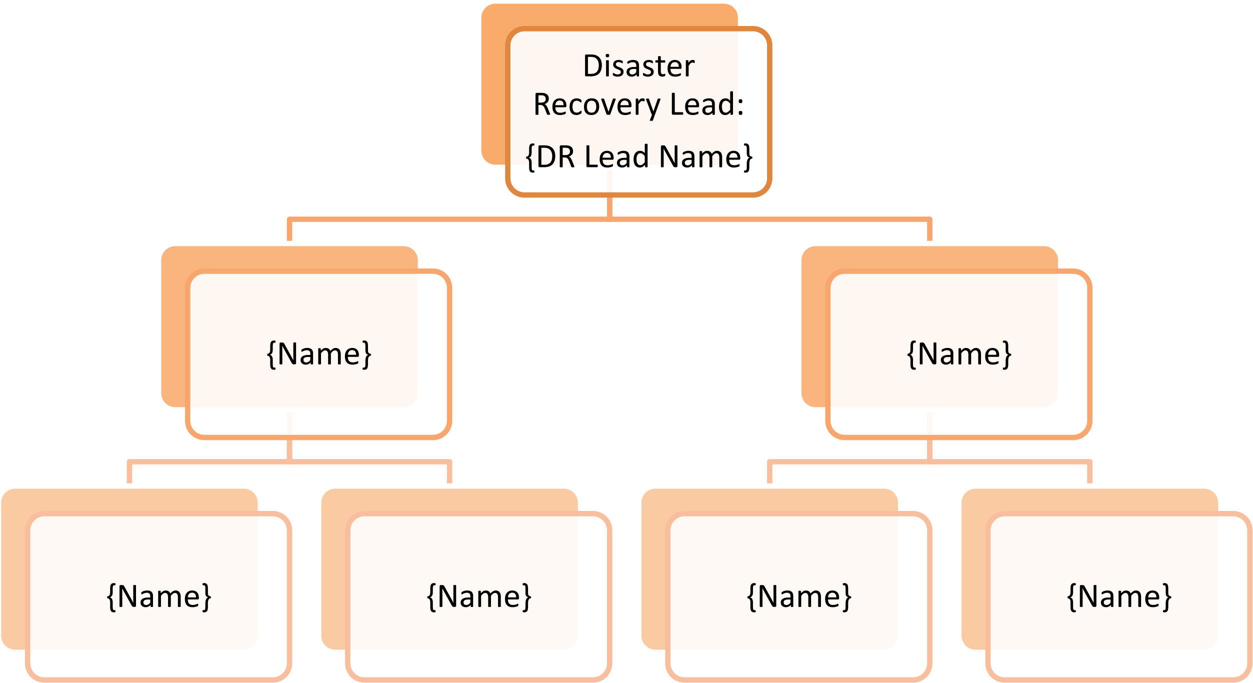
EXTERNAL CONTACTS

First Name	Last Name	Title	Contact Type	Contact information
Property Manager / Landlord				
Account #:				
			Work	
			Mobile	
			Email	
Power Company				
Account #:				
			Work	
			Mobile	
			Email	
Security Company				
Account #:				
			Work	
			Mobile	
			Email	
Network Provider				
Account #:				
			Work	
			Mobile	
			Email	
Telecom Carrier				
Account #:				
			Work	
			Mobile	

			Email	
Managed Services / Help Desk				
Account #:				
			Work	
			Mobile	
			Email	
Server Supplier				
Account #:				
			Work	
			Mobile	
			Email	
Workstation Supplier				
Account #:				
			Work	
			Mobile	
			Email	
Insurance				
Account #:				
			Work	
			Mobile	
			Email	
Off-site Storage				
Account #:				
			Work	
			Mobile	
			Email	

Power Generator				
Account #:				
			Work	
			Mobile	
			Email	
Other				
Account #:				
			Work	
			Mobile	
			Email	

NOTIFICATION NETWORK



SCOPE

Required

The {Organization Name} DR Plan takes all of the following technology areas into consideration:

- Edit this list to reflect your organization
- *Network Infrastructure*
- *Servers Infrastructure*
- *Telephony System*
- *Data Storage and Backup Systems*
- *Data Output Devices*
- *End-user Computers*
- *Organizational Software Systems*
- *Database Systems*
- *IT Documentation*

This DR Plan does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters.

VERSION INFORMATION & CHANGES

Required

Any changes, edits and updates made to the DR Plan will be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DR Plan are up to date. Whenever there is an update to the DR Plan, {Organization Name} requires that the version number be updated to indicate this.

Add rows as required as the DR Plan is amended.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
Bob Jones	*DR Lead*	*01/01/14*	*1.0*	*Initial version of DR Plan*
Bob Jones	*DR Lead*	*01/01/15*	*2.0*	*Revised to include new Evolve IP availability zones*
Lisa Smith	*CEO*	*04/03/15*	*2.1*	*Replaced Bob Jones as DR Lead*

DISASTER RECOVERY TEAMS & RESPONSIBILITIES

Required

In the event of a disaster, different teams will be required to assist the IT department in their effort to restore normal functionality to the employees of {Organization Name}. The different teams and their responsibilities are as follows:

- Edit this list to reflect your organization
- *Disaster Recovery Lead(s)*
- *Disaster Management Team*
- *Network Team*
- *Server Team*
- *Applications Team*

The lists of roles and responsibilities in this section have been created by {Organization Name} and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

The following teams will vary depending on the size of your organization. Some teams/roles may be combined or may be split into more than one team.

DISASTER RECOVERY LEAD

Required

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at {Organization Name}, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased. As a result, the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in {Organization Name}.

ROLE AND RESPONSIBILITIES

- Edit this list to reflect your organization
- *Make the determination that the organization is declaring that a disaster has occurred and trigger the DR Plan and related processes.*
- *Initiate the DR Notification Network.*
- *Be the single point of contact for and oversee all of the DR Teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DR Plan test and author all DR Plan updates.*

CONTACT INFORMATION

Add or delete rows to reflect the size the Disaster Recovery Team in your organization.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Lisa Smith	*Primary Disaster Lead*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Bob Jones	*Secondary Disaster Lead*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Evolve IP	*Managed IT*	*877.459.4347 x5*		

DISASTER MANAGEMENT TEAM

OPTIONAL

The Disaster Management Team that will oversee the entire disaster recovery process and will be the first team required to take action in the event of a disaster. This team will evaluate the disaster and determine the steps required to get the organization back to business as usual.

In a small organization, these roles may be performed by the Disaster Recovery Lead.

ROLE & RESPONSIBILITIES

- Edit this list to reflect your organization
- *Set the DR Plan into motion after the Disaster Recovery Lead has declared a disaster*
- *Determine the magnitude and class of the disaster*
- *Determine what systems and processes have been affected by the disaster*
- *Communicate the disaster to the other disaster recovery teams*
- *Determine what first steps need to be taken by the disaster recovery teams*
- *Keep the disaster recovery teams on track with pre-determined expectations and goals*
- *Keep a record of money spent during the disaster recovery process*
- *Ensure that all decisions made abide by the DR Plan and policies set by* {Organization Name}
- *Get the secondary site ready to restore business operations*
- *Ensure that the secondary site is fully functional and secure*
- *Create a detailed report of all the steps undertaken in the disaster recovery process*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored*
- *After* {Organization Name} *is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

CONTACT INFORMATION

Add or delete rows to reflect the size the Disaster Management Team in your organization.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Lisa Smith	*“Regular” title*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Bob Jones	*“Regular” title*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Evolve IP	*Managed IT*	*877.459.4347 x5*		

NETWORK TEAM

Required

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the organization as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

ROLE & RESPONSIBILITIES

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to / from Evolve IP availability zones, the team will determine which network services are not functioning at the primary availability zones*
- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.*
- *In the event of a disaster that does require migration to Evolve IP availability zones the team will ensure that all network services are brought online at the secondary availability zones*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
    - *All members of the DR Teams*
    - *All C-level and Executive Staff*
    - *All IT employees*
    - *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby availability zone*
- *Install and implement any tools, hardware, software and systems required in the primary availability zone*
- *After* {Organization Name} *is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

CONTACT INFORMATION

Add or delete rows to reflect the size of the Network Team in your organization.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Lisa Smith	*Network Manager*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Bob Jones	*Network Administrator*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Evolve IP	*Managed IT*	*877.459.4347 x5*		

SERVER TEAM

Required

The Server Team will be responsible for providing the physical server infrastructure required for the organization to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

ROLE & RESPONSIBILITIES

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to / from Evolve IP availability zones, the team will determine which servers are not functioning at the primary availability zone*
- *If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - *Assess the damage to any servers*
  - *Restart and refresh servers if necessary*
- *Ensure that secondary servers located in Evolve IP availability zones are kept up-to-date with system patches*
- *Ensure that secondary servers located in Evolve IP availability zones are kept up-to-date with application patches*
- *Ensure that secondary servers located in Evolve IP availability zones are kept up-to-date with data copies*
- *Ensure that the secondary servers located in the standby availability zones are backed up appropriately*
- *Ensure that all of the servers in the standby availability zones abide by* {Organization Name}*'s server policy*
- *Install and implement any tools, hardware, and systems required in the standby availability zones*
- *Install and implement any tools, hardware, and systems required in the primary availability zones*
- *After* {Organization Name} *is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

CONTACT INFORMATION

Add or delete rows to reflect the size of the Server Team in your organization.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Mandy Bell	*Operations Manager*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Matthew Davis	*Systems Administrator*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Evolve IP	*Managed IT*	*877.459.4347 x5*		

APPLICATIONS TEAM

Required

The Applications Team will be responsible for ensuring that all organization applications operate as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

ROLE & RESPONSIBILITIES

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to / from Evolve IP availability zones, the team will determine which applications are not functioning at the primary availability zones*
- *If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:*
    - *Assess the impact to application processes*
    - *Restart applications as required*
    - *Patch, recode or rewrite applications as required*
- *Ensure that secondary servers located in Evolve IP availability zones are kept up-to-date with application patches*
- *Ensure that secondary servers located in Evolve IP availability zones are kept up-to-date with data copies*
- *Install and implement any tools, software and patches required in the standby availability zones*
- *Install and implement any tools, software and patches required in the primary availability zones*
- *After* {Organization Name} *is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

CONTACT INFORMATION

Add or delete rows to reflect the size of the Application Team in your organization.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Jack Rand	*Program Manager*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Gary White	*Systems Administrator*	*555-555-5555*	*555-555-5555*	*555-555-5555*
Evolve IP	*Managed IT*	*877.459.4347 x5*		

DATA AND BACKUPS

Required

This section explains where all of the organization’s data resides as well as where it is backed up. Use this information to locate and restore data in the event of a disaster.

In this section it is important to explain where the organization’s data resides. Discuss the location of all the organization’s servers, backups and offsite backups and list what information is stored on each of these.

DATA IN ORDER OF CRITICALITY

Please list all of the data in your organization in order of their criticality. Add or delete rows as needed to the table below.

Rank	Data	Data Type	Back-up Frequency	Backup Location(s) / Evolve IP Backup Product (Cloud Backup / Reflection)
1	{Data Name or Group}	{Confidential, Public, Personally identifying information}	{Frequency that data is backed up}	{Where data is backed up}
2				
3				
4				
5				
6				
7				
8				
9				
10				

RESTORING IT FUNCTIONALITY

Required

Should a disaster actually occur and {Organization Name} need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which {Organization Name}'s information system will be recovered.

This section will contain all of the information needed for the organization to get back to its regular functionality after a disaster has occurred. It is important to include all Standard Operating Procedures documents, run-books, network diagrams, software format information etc. in this section.

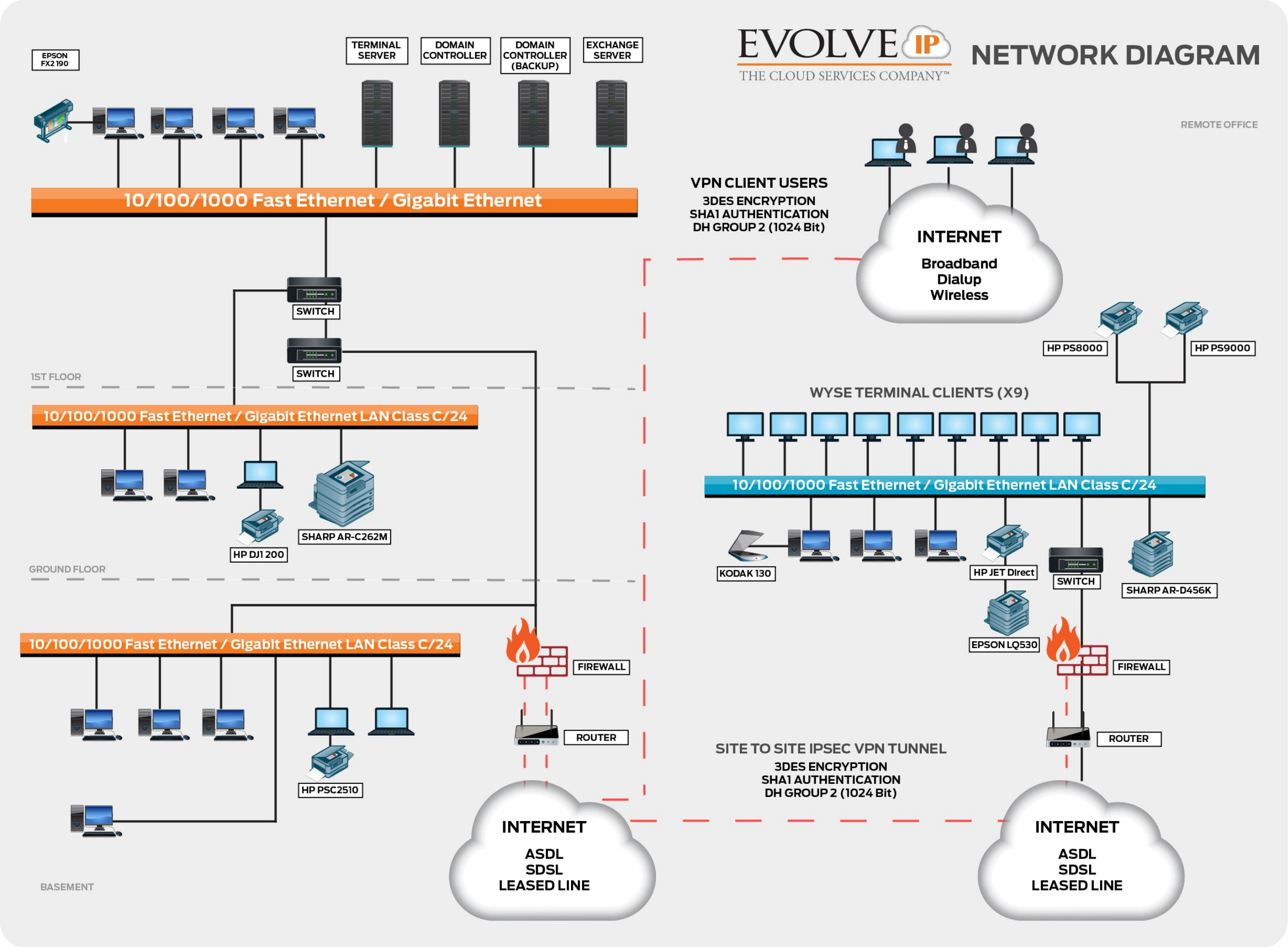
CURRENT SYSTEM ARCHITECTURE

Required

In this section, include a detailed system architecture diagram. Ensure that all of the organization's systems and their locations are clearly indicated.

{System Architecture Diagram}

Example:



IT SYSTEMS

Please list all of the IT Systems in your organization in order of their criticality. Next, list each system's components that will need to be brought back online in the event of a disaster. Add or delete rows as needed to the table below.

Rank	IT System	System Components (In order of importance)
1		
1		
1		
2		
2		
2		
3		
3		
3		
4		

CONNECTIVITY

Provider	Circuit Type	Bandwidth	CPE	CPE Gear Model	Address, City State ZIP	Onsite Location	Notes
Cogent	*Internet*	*1 Gbps*	*No*		*989 Old Eagle School, Wayne PA 19087*	*Network Closet Floor 1 Rack 2 Slot 40*	*Primary Internet circuit*
Level 3	*MPLS*	*50 Mbps*	*Yes*	*Cisco 3750*	*989 Old Eagle School, Wayne PA 19087*	*Network Closet Floor 1 Rack 2 Slot 38*	*Connection to Ohio Office*
Cogent	*Internet*	*10MB*	*No*		*989 Old Eagle School, Wayne PA 19087*	*Network Closet Floor 1 Rack 2 Slot 37*	*Backup Internet connectivity*

NETWORK EQUIPMENT

SWITCHES

Make/Model	Description	MGMT IP	Misc. Details

ROUTERS

Make/Model	Description	MGMT IP	Misc. Details

LOAD BALANCERS

Make/Model	Description	MGMT IP	VIP Details

VPN DEVICES

Make/Model	Description	MGMT IP	Tunnel Details

FIREWALLS

Make/Model	Description	MGMT IP	Notes

MISCELLANEOUS NETWORK APPLIANCES

Make/Model	Description	MGMT IP	Notes

SERVERS

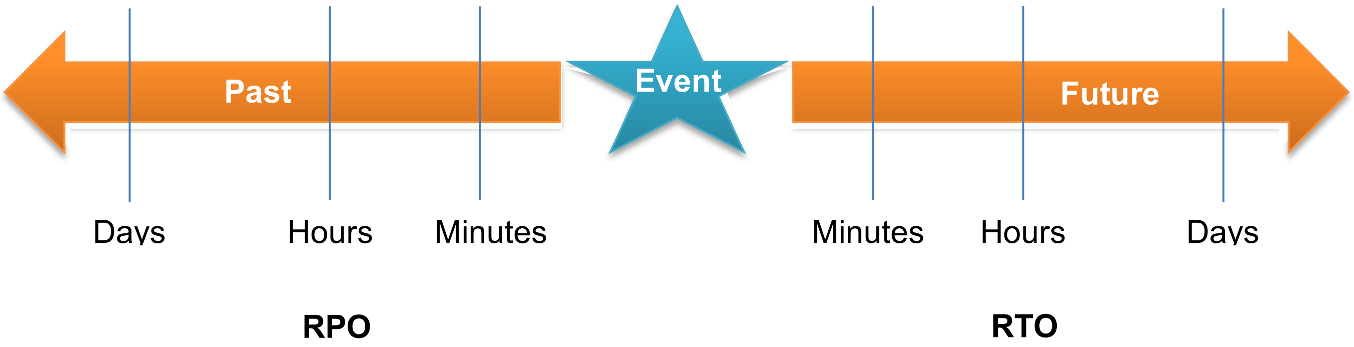
Note: (Rank of “1” = most important)

Name	Rank	Type	VM or PHY	CPU	RAM	Disk	OS Version	Purpose

SEVERITY ONE SYSTEM

When determining the right Disaster Recovery services for your organization, there are three aspects to consider:

- **Source of System** – Whether your system is onsite, in the Evolve IP Cloud, or elsewhere.
- **Recovery Point Objective (RPO)** – How current your data is at the recovery site.
- **Recovery Time Objective (RTO)** – How long it should take to bring an environment back online once a disaster or major incident is declared.



In this section you will be required to rank each system's components in order of severity, supplying the information that each system will require to bring it back online.

EXAMPLE:

System Name	{State the name of the System here}
Server Name	{State the name of the specific server here}
Recovery Time Objective	{State the IT Component's Recovery Time Objective here}
Recovery Point Objective	{State the IT Component's Recovery Point Objective here}
Replication Target Site	Evolve IP East / West
Replication Technology	DRaaS ZT
Backup Target	Evolve IP Cloud Backup or Reflection
Backup Job Frequency	Nightly
Last Restore Test	

PROCEDURE

The following are the steps associated with bringing {Component Name} back online in the event of a disaster or system failure.

Step	Action	Responsibility
1	{Step 1 Action}	**{Person/group responsible}**
2		
3		
4		
5		

SEVERITY TWO SYSTEM

Repeat as above as needed for as many systems as the organization makes use of.

PLAN TESTING & MAINTENANCE

Required

While efforts will be made initially to construct this DR Plan is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the organization will change. As a result of these two factors this plan will need to be tested.

MAINTENANCE

Required

The DR Plan will be updated {indicate frequency} or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- Edit this list as required

1. *Ensuring that all team lists are up to date*
2. *Reviewing the plan to ensure that all of the instructions are still relevant to the organization*
3. *Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals*
4. *Ensuring that the plan meets any requirements specified in new laws*

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

TESTING

Required

{Organization Name} is committed to ensuring that this DR Plan is functional. The DR Plan should be tested every {indicate frequency} in order to ensure that it is still effective. Testing the plan will be carried out as follows:

Select which method(s) your organization will employ to test the DR Plan

1) **DR Rehearsal:** Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DR Plan Lead to make appropriate changes to the plan. Staff should be familiar with procedures, equipment, and all Evolve IP availability zones (if required).
2) **Failover Testing:** Under this scenario, servers and applications are brought online in an isolated environment. There's no impact to existing operations or uptime. Systems administrators ensure that all operating systems come up cleanly. Application administrators validate that all applications perform as expected.
3) **Live-Failover Testing:** A live-failover test activates the total DR Plan. The test will disrupt normal operations, and therefore should be approached with caution. Ensure you have completed several iterations of steps 1 and 2 before proceeding with this step. Additionally, communicate all expected disruptions well in advance of performing this test.

Any gaps in the DR Plan that are discovered during the above phases will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

BUSINESS PROCESS/FUNCTION RECOVERY COMPLETION FORM

The DR Lead is responsible for completing and signing this form for each process recovered. Please use a separate form for each recovered business process.

NAME OF BUSINESS PROCESS:	
Completion Date of Work by DR Team	{ENTER DATE HERE}
Date of Transition Back to Business Unit Management	{ENTER DATE HERE}

I confirm that the work of the Disaster Recovery Team has been completed in accordance with the DR Plan for the above process and that normal business operations have been effectively restored.

DR Team Lead Name: ____

Signature: ____

Date: ______________________________

Comments:

I confirm that above business process is now acceptable for normal working conditions.

DR Team Lead Name: ____

Title: ____

Signature: ____

Date: ______________________________